

WHAT IS CLAIMED IS:

1 1. A method for thwarting coordinated SYN denial of service (CSDoS)
2 attacks against a server S disposed in a network of interconnected elements
3 communicating using the TCP protocol, comprising the steps of
4 controlling a network switch to divert a predetermined fraction of SYN packets
5 destined for said server, to a web guard processor,
6 establishing a first TCP connection between one or more clients originating said
7 packets and said web guard processor, and a second TCP connection between said web
8 guard processor and said server, so that packets can be transmitted between said one or
9 more clients and said server,
10 monitoring the number of timed-out connections between said web guard server
11 and said one or more clients,
12 if the number of timed-out connections between said web guard server and said
13 one or more clients exceeds a first predetermined threshold, controlling said switch to
14 divert all SYN packets destined to said server to said web guard processor.

1 2. The method of claim 1 wherein said process further includes generating an
2 alarm indicating that said server is likely to be under attack.

1 3. The method of claim 1 including the further steps of
2 determining if the number of timed-out connections between said web guard server
3 and said clients exceeds a second predetermined threshold, and
4 if so, controlling said switch to delete all SYN packets destined for said server.

1 4. The method of claim 3 wherein said process further includes generating an
2 alarm indicating that said server is under attack.

1 5. The method of claim 1 further including the step of notifying said server
2 that it is under attack.

Sub
Att
"SECRET"

7. A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server S disposed in a network of interconnected elements communicating using the TCP protocol, said attack originating from a malicious host generating SYN packets destined for said server, said method comprising the steps of arranging a switch receiving said SYN packets destined to said server to forward

1 8. A method for thwarting coordinated SYN denial of service (CSDoS)
2 attacks against a server S disposed in a network of interconnected elements
3 communicating using the TCP protocol, comprising the steps of
4 forwarding a statistical sampling of said packets from a switch in said network to a
5 processor,

1 9. The method of claim 8 wherein said switch is arranged to discard packets in
2 the event an attack is detected.